Biometrics

Evaluation Letter

2020/12/01

To whom it may concern:

The Swiss Center for Biometrics Research and Testing (SCBRT) is part of the Biometrics Security and Privacy group at the Idiap Research Institute. The SCBRT is also a FIDO Alliance Accredited Biometrics Laboratory (ABL). On behalf of Identy Inc., the SCBRT has conducted an evaluation of the presentation attack detection (PAD) efficacy of the Identy Face Authentication solution in accordance with ISO/IEC 30107-3 evaluation protocols. This letter describes the evaluation and summarizes the main outcomes.

Target Of Evaluation (TOE): Identy Face Authentication solution, version 1.9.4.0.

Test Harness: Motorola g7 smartphone, running Android 9. The TOE uses the front camera of the smartphone to capture face biometric-samples.

Scope of Evaluation: PAD, using Level A attacks only. The Presentation Attack Instruments (PAI) have been created in accordance with ISO standards used to assess and triage the attack potential of presentation attacks (PA). Level A PAs are attacks that can be easily created within a day, requiring neither sophisticated equipment nor a high degree of expertise.

PAIs of the following four Level A species have been used in this study:

- two PAI species representing printed-photo attacks, using face images printed on two kinds of photo-quality paper (matte and glossy) on a color laser printer, and
- two PAI species of replay-attacks, based on faces displayed on two devices with different screen sizes.

The TOE has been evaluated using *bona fide* and PA transactions, where each transaction consists of up to five attempts (each attempt being a single presentation) performed within a period of 30 seconds.

Ten subjects participated in this evaluation (four female and six male). Each subject first enrolled oneself, and then performed five *bona fide* transactions. Subsequently, five PA transactions were made for each PAI (10 PAIs per species).

The performance metrics estimated in this evaluation are summarized in Table 1.

Metric	**Value**	**Explanation**
BPCER	8%	Bona-fide Presentation Classification Error Rate (BPCER) is the proportion of *bona fide* transactions that were incorrectly rejected by the PAD subsystem of the TOE.
APCER	0%	Attack Presentation Classification Error Rate (APCER) is the proportion of PAs that were incorrectly classified as *bona fide* by the PAD subsystem of the TOE.
IAPMR	0%	Impostor Attack Presentation Match Rate (IAPMR) estimates the vulnerability of the TOE to PAs and is computed as the proportion of PAs on a given identity that were accepted by the TOE.

Table 1: Performance metrics estimated for the TOE in this evaluation.

Additional Analysis: The TOE records the capture-time for each attempt, that is, the time required to capture the biometrics sample, as well as the processing time required to generate a decision based on the captured biometric sample. The median capture-time per attempt was about 4 seconds. The median processing-time (after the biometric sample was captured) including PAD and face-recognition, was about 230 milliseconds.

Sincerely yours,

Dr. Sébastien Marcel

Dr. François Foglia
Deputy Director
Idiap Research Institute